

Department of Justice

§ 25.7

have been searched and one matching record was found.

(4) Multiple matching record response, if all records in the relevant databases have been searched and more than one matching record was found.

(g) Generally, based on the response(s) provided by the NICS, and other information available in the state and local record systems, a POC will:

(1) Confirm any matching records; and

(2) Notify the FFL that the transfer may proceed, is delayed pending further record analysis, or is denied. "Proceed" notifications made within three business days will be accompanied by the NTN or STN traceable to the NTN. The POC may or may not provide a transaction number (NTN or STN) when notifying the FFL of a "Denied" response.

(h) *POC Determination Messages.* POCs shall transmit electronic NICS transaction determination messages to the FBI for the following transactions: open transactions that are not resolved before the end of the operational day on which the check is requested; denied transactions; transactions reported to the NICS as open and later changed to proceed; and denied transactions that have been overturned. The FBI shall provide POCs with an electronic capability to transmit this information. These electronic messages shall be provided to the NICS immediately upon communicating the POC determination to the FFL. For transactions where a determination has not been communicated to the FFL, the electronic messages shall be communicated no later than the end of the operational day on which the check was initiated. With the exception of permit checks, newly created POC NICS transactions that are not followed by a determination message (deny or open) before the end of the operational day on which they were initiated will be assumed to have resulted in a proceed notification to the FFL. The information provided in the POC determination messages will be maintained in the NICS Audit Log described in §25.9(b). The NICS will destroy its records regarding POC determinations in accordance with the procedures detailed in §25.9(b).

(i) *Response recording.* FFLs are required to record the system response, whether provided by the FBI NICS Operations Center or a POC, on the appropriate ATF form for audit and inspection purposes, under 27 CFR part 178 recordkeeping requirements. The FBI NICS Operations Center response will always include an NTN and associated "Proceed," "Delayed," or "Denied" determination. POC responses may vary as discussed in paragraph (g) of this section. In these instances, FFLs will record the POC response, including any transaction number and/or determination.

(j) *Access to the NICS Index for purposes unrelated to NICS background checks required by the Brady Act.* Access to the NICS Index for purposes unrelated to NICS background checks pursuant to 18 U.S.C. 922(t) shall be limited to uses for the purpose of:

(1) Providing information to Federal, state, or local criminal justice agencies in connection with the issuance of a firearm-related or explosives-related permit or license, including permits or licenses to possess, acquire, or transfer a firearm, or to carry a concealed firearm, or to import, manufacture, deal in, or purchase explosives; or

(2) Responding to an inquiry from the ATF in connection with a civil or criminal law enforcement activity relating to the Gun Control Act (18 U.S.C. Chapter 44) or the National Firearms Act (26 U.S.C. Chapter 53).

[Order No. 2186-98, 63 FR 58307, Oct. 30, 1998, as amended by Order No. 2727-2004, 69 FR 43900, July 23, 2004]

§ 25.7 Querying records in the system.

(a) The following search descriptors will be required in all queries of the system for purposes of a background check:

- (1) Name;
- (2) Sex;
- (3) Race;
- (4) Complete date of birth; and
- (5) State of residence.

(b) A unique numeric identifier may also be provided to search for additional records based on exact matches by the numeric identifier. Examples of unique numeric identifiers for purposes of this system are: Social Security number (to comply with Privacy Act

§ 25.8

requirements, a Social Security number will not be required by the NICS to perform any background check) and miscellaneous identifying numbers (e.g., military number or number assigned by Federal, state, or local authorities to an individual's record). Additional identifiers that may be requested by the system after an initial query include height, weight, eye and hair color, and place of birth. At the option of the querying agency, these additional identifiers may also be included in the initial query of the system.

§ 25.8 System safeguards.

(a) Information maintained in the NICS Index is stored electronically for use in an FBI computer environment. The NICS central computer will reside inside a locked room within a secure facility. Access to the facility will be restricted to authorized personnel who have identified themselves and their need for access to a system security officer.

(b) Access to data stored in the NICS is restricted to duly authorized agencies. The security measures listed in paragraphs (c) through (f) of this section are the minimum to be adopted by all POCs and data sources having access to the NICS.

(c) State or local law enforcement agency computer centers designated by a Control Terminal Agency as POCs shall be authorized NCIC users and shall observe all procedures set forth in the NCIC Security Policy of 1992 when processing NICS background checks. The responsibilities of the Control Terminal Agencies and the computer centers include the following:

(1) The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

(2) Since personnel at these computer centers can have access to data stored in the NICS, they must be screened thoroughly under the authority and supervision of a state Control Terminal Agency. This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center

28 CFR Ch. I (7-1-14 Edition)

being serviced through a state Control Terminal Agency. This screening will also apply to non-criminal justice maintenance or technical personnel.

(3) All visitors to these computer centers must be accompanied by staff personnel at all times.

(4) POCs utilizing a state/NCIC terminal to access the NICS must have the proper computer instructions written and other built-in controls to prevent data from being accessible to any terminals other than authorized terminals.

(5) Each state Control Terminal Agency shall build its data system around a central computer, through which each inquiry must pass for screening and verification.

(d) Authorized state agency remote terminal devices operated by POCs and having access to the NICS must meet the following requirements:

(1) POCs and data sources having terminals with access to the NICS must physically place these terminals in secure locations within the authorized agency;

(2) The agencies having terminals with access to the NICS must screen terminal operators and must restrict access to the terminals to a minimum number of authorized employees; and

(3) Copies of NICS data obtained from terminal devices must be afforded appropriate security to prevent any unauthorized access or use.

(e) FFL remote terminal devices may be used to transmit queries to the NICS via electronic dial-up access. The following procedures will apply to such queries:

(1) The NICS will incorporate a security authentication mechanism that performs FFL dial-up user authentication before network access takes place;

(2) The proper use of dial-up circuits by FFLs will be included as part of the periodic audits by the FBI; and

(3) All failed authentications will be logged by the NICS and provided to the NICS security administrator.

(f) FFLs may use the telephone to transmit queries to the NICS, in accordance with the following procedures: